AMEDMENTS

In The Claims:

Please amend the claims as follows:

Claim 1. (currently amended) A portable computer equipped with an embedded controller (EC), the EC being equipped with a security mechanism operable with a method comprising steps of:

providing at least one key that provides a key signal to allow the EC to learn whether the portable computer is to be locked;

turning on the security mechanism while the EC receives the key signal indicating that the portable computer is to be locked;

determining ~~only~~ by the EC whether a hacking action is taking place; and

activating a security action in responding to the hacking action.

Claim 2. (currently amended) The portable computer of claim 1, wherein the ~~security mechanism~~ step of turning on the security mechanism further comprises a step of preventing ~~prevents~~ the portable computer from being turned on.

Claim 3. (currently amended) The portable computer of claim 1, wherein the ~~security mechanism~~ step of turning on the security mechanism further comprises a step of preventing ~~prevents~~ an input from a keyboard.

Claim 4. (currently amended) The portable computer of claim 1, wherein the ~~security mechanism~~ step of turning on the security mechanism further comprises a step of preventing ~~prevents~~ an input from a mouse.

Claim 5. (currently amended) The portable computer of claim 1, wherein the ~~security mechanism~~ step of turning on the security mechanism further comprises a step of preventing ~~prevents~~ a basic input/output system (BIOS) data from being changed.

Claim 6. (currently amended) The portable computer of claim 1, wherein the key is an internal unit ~~device~~ or an internal function of the portable computer.

Claim 7. (currently amended) The portable computer of claim 1, wherein the key is an unit or a function of an external device ~~or an external function of the portable computer~~.

Claim 8. (previously presented) The portable computer of claim 1, wherein the key signal is a binary signal.

Claim 9. (currently amended) The portable computer of claim 1, wherein the security action further comprises a related follow-up procedure of a security function ~~takes place~~ when a hacking action is detected by the security mechanism.

Claim 10. (previously presented) The portable computer of claim 9, wherein the

related follow-up procedure turns off the portable computer.

Claim 11. (previously presented) The portable computer of claim 9, wherein the related follow-up procedure turns off a monitor device of the portable computer.

Claim 12. (previously presented) The portable computer of claim 9, wherein the related follow-up procedure executes a security program.

Claim 13. (currently amended) An embedded controller (EC) equipped to a portable computer, the EC being operable with a security mechanism operable with a method comprising steps of:

providing at least one key that provides a key signal to allow the EC to learn whether the portable computer is to be locked;

turning on the security mechanism while the EC receives the key signal indicating that the portable computer is to be locked;

determining ~~only~~ by the EC whether a hacking action is taking place; and

activating a security action in responding to the hacking action.

Claim 14. (currently amended) A security mechanism for a portable computer, the security mechanism being equipped to an embedded controller that is equipped to a portable the security mechanism running a process comprising:

providing at least one key that provides a key signal to allow the EC to learn whether the portable computer is to be locked;

turning on the security mechanism while the EC receives the key signal indicating that the portable computer is to be locked;

determining ~~only~~ by the EC whether a hacking action is taking place; and

activating a security action in responding to the hacking action.

Claim 15. (new) The portable computer of claim 7, wherein the external device includes an infrared remote control device.